Family list
1 family member for:
JP2001249941
Derived from 1 application.

1 **DATA BASE ACCESS CONTROL METHOD, DATA BASE DEVICE AND RECORDING MEDIUM HAVING DATA BASE CONTROL PROGRAM RECORDED THEREON**
Publication info: **JP2001249941 A** - 2001-09-14

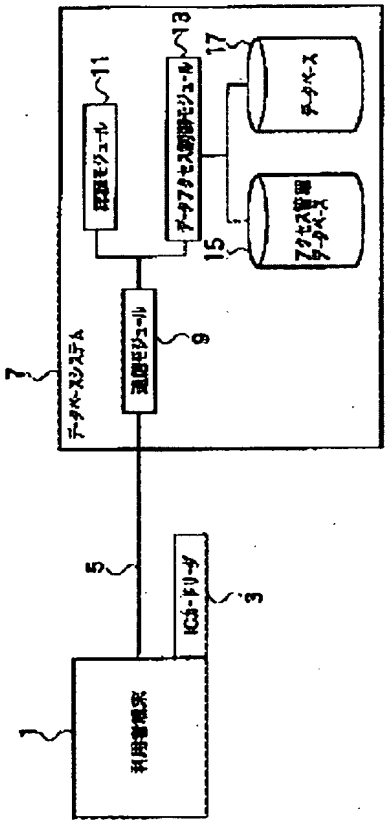
Data supplied from the ***esp@cenet*** database - Worldwide

DATA BASE ACCESS CONTROL METHOD, DATA BASE DEVICE AND RECORDING MEDIUM HAVING DATA BASE CONTROL PROGRAM RECORDED THEREON

Patent number: JP2001249941
Publication date: 2001-09-14
Inventor: SUDO TOMOKO; KUBOTA YUKIHIRO; TSUBOI TOSHIAKI; NAKAMURA YOSHIAKI; HASHIMOTO SATOSHI; SAWACHI MAMORU
Applicant: NIPPON TELEGRAPH & TELEPHONE
Classification:
- international: G06F17/30; G06F12/00; G06F12/14; G06F15/00
- european:
Application number: JP20000060985 20000306
Priority number(s): JP20000060985 20000306

Abstract of **JP2001249941**

PROBLEM TO BE SOLVED: To provide a data base access control method, a data base device and a recording medium having a data base control program recorded thereon capable of accurately preventing the leakage of the data of a data access object by using both of first authentication information for authenticating an accessing person like a doctor for instance and second authentication information for authenticating the data access object like a patient. SOLUTION: The first authentication information is transmitted from a terminal to a data base, the data base authenticates the authentication information and returns an authentication result to the terminal. The terminal transmits the second authentication information to the data base together with data specifying information. The data base authenticates the authentication information, judges the propriety of access to the data specified by the data specifying information on the basis of the authentication result and the data specifying information and permits the access to the data specified by the data specifying information in the case that the access is approved.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－249941
（P2001－249941A）
(43)公開日　平成13年９月14日(2001.9.14)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ	17/30	１２０	Ｇ０６Ｆ 17/30	１２０Ｂ	５Ｂ０１７
		１１０		１１０Ｆ	５Ｂ０７５
	12/00	５３１	12/00	５３１Ａ	５Ｂ０８２
	12/14	３１０	12/14	３１０Ｋ	５Ｂ０８５
	15/00	３３０	15/00	３３０Ｄ	

審査請求　未請求　請求項の数11　ＯＬ　（全 16 頁）

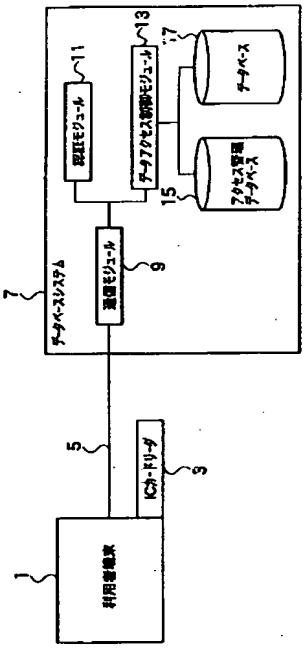
(21)出願番号　特願2000－60985(P2000－60985)
(22)出願日　平成12年３月６日(2000.3.6)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　須藤　朋子
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　久保田　幸宏
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

最終頁に続く

(54)【発明の名称】　データベースアクセス制御方法およびデータベース装置とデータベース制御プログラムを記録した記録媒体

(57)【要約】
【課題】　例えば医師のようなアクセス者を認証する第１の認証情報と患者のようなデータアクセス対象を認証する第２の認証情報の両認証情報を用いて、データアクセス対象のデータの漏洩を適確に防止し得るデータベースアクセス制御方法およびデータベース装置とデータベース制御プログラムを記録した記録媒体を提供する。
【解決手段】　端末から第１の認証情報をデータベースに送信し、データベースは該認証情報を認証し、認証結果を端末に返送し、端末はデータ指定情報とともに第２の認証情報をデータベースに送信し、データベースは該認証情報を認証し、該認証結果とデータ指定情報に基づきデータ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、データ指定情報で指定されるデータへのアクセスを許可する。



【特許請求の範囲】

【請求項１】　端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベースアクセス制御方法であって、
端末からアクセス者を認証する第１の認証情報をデータベース装置に送信し、
データベース装置は受信した第１の認証情報を認証して、その認証結果を端末に返送し、
端末は受信した認証結果に基づき所望のデータへのアクセスを要求すべく該データを指定するデータ指定情報とともにデータアクセス対象を認証する第２の認証情報をデータベース装置に送信し、
データベース装置は受信した第２の認証情報を認証し、この認証結果と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記データ指定情報で指定されるデータへのアクセスを許可することを特徴とするデータベースアクセス制御方法。

【請求項２】　端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベースアクセス制御方法であって、
端末からアクセス者を認証する第１の認証情報およびデータアクセス対象を認証する第２の認証情報をデータベース装置に送信し、
データベース装置は受信した第１の認証情報を認証して、第１の認証情報と第２の認証情報を対にして格納し、
端末から所望のデータへのアクセスを要求すべく該データを指定するデータ指定情報とともに第１の認証情報およびデータアクセス対象情報をデータベース装置に送信し、
データベース装置は受信した第１の認証情報で前記格納された第１および第２の認証情報の対を参照し、前記受信したデータアクセス対象が第１の認証情報に対して対として格納されている第２の認証情報で認証されるものであるか否かを判定し、該データアクセス対象が第２の認証情報で認証されるものである場合、第１および第２の認証情報と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記データ指定情報で指定されるデータへのアクセスを許可することを特徴とするデータベースアクセス制御方法。

【請求項３】　前記データ指定情報で指定されるデータへのアクセスの可否を判定する処理は、該データ指定情報に対応して該データへのアクセスを許可するアクセス者を指定するアクセス者指定データおよびデータアクセス対象を指定するデータアクセス対象指定データを格納していることを特徴とする請求項１または２記載のデータベースアクセス制御方法。

【請求項４】　前記端末からアクセス者を認証する第１の認証情報をデータベース装置に送信する処理は、ＩＣカードに格納されている第１の認証情報を読み出してデータベース装置に送信し、
前記端末からデータアクセス対象を認証する第２の認証情報をデータベース装置に送信する処理は、ＩＣカードに格納されている第２の認証情報を読み出してデータベース装置に送信することを特徴とする請求項１または２記載のデータベースアクセス制御方法。

【請求項５】　端末は、前記データ指定情報で指定されるデータへのアクセスを許可された場合、該データ指定情報で指定されるデータに対するデータの変更、追加登録、読み出しを行うことができることを特徴とする請求項１または２記載のデータベースアクセス制御方法。

【請求項６】　端末からのアクセス者に対して格納しているデータを提供するデータベース装置であって、
端末から送信されるアクセス者を認証する第１の認証情報を受信して認証し、この認証結果を端末に返送する認証手段と、
端末からデータを指定するデータ指定情報とともに送信されてくるデータアクセス対象を認証する第２の認証情報を受信し、この受信した第２の認証情報を認証し、この認証結果と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可するアクセス許可手段とを有することを特徴とするデータベース装置。

【請求項７】　端末からのアクセス者に対して格納しているデータを提供するデータベース装置であって、
端末から送信されるアクセス者を認証する第１の認証情報およびデータアクセス対象を認証する第２の認証情報を受信し、この受信した第１の認証情報を認証し、第１の認証情報と第２の認証情報を対にして格納する格納手段と、
端末からデータを指定するデータ指定情報とともに送信されてくる第１の認証情報およびデータアクセス対象情報を受信し、この受信した第１の認証情報で前記格納手段に格納されている第１および第２の認証情報の対を参照し、前記受信したデータアクセス対象が第１の認証情報に対して対として格納されている第２の認証情報で認証されるものであるか否かを判定し、該データアクセス対象が第２の認証情報で認証されるものである場合、第１および第２の認証情報と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可するアクセス許可手段とを有することを特徴とするデータベース装置。

【請求項８】　前記アクセス許可手段は、前記データ指定情報に対応して該データへのアクセスを許可するアク

セス者を指定するアクセス者指定データおよびデータアクセス対象を指定するデータアクセス対象指定データを蓄積する蓄積手段を有することを特徴とする請求項６または７記載のデータベース装置。

【請求項９】　端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベース制御プログラムを記録した記録媒体であって、

端末から送信されるアクセス者を認証する第１の認証情報を受信して認証し、この認証結果を端末に返送し、

端末からデータを指定するデータ指定情報とともに送信されてくるデータアクセス対象を認証する第２の認証情報を受信し、この受信した第２の認証情報を認証し、この認証結果と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可することを特徴とするデータベース制御プログラムを記録した記録媒体。

【請求項１０】　端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベース制御プログラムを記録した記録媒体であって、

端末から送信されるアクセス者を認証する第１の認証情報およびデータアクセス対象を認証する第２の認証情報を受信し、この受信した第１の認証情報を認証し、第１の認証情報と第２の認証情報を対にして格納し、

端末からデータを指定するデータ指定情報とともに送信されてくる第１の認証情報およびデータアクセス対象情報を受信し、この受信した第１の認証情報で前記格納されている第１および第２の認証情報の対を参照し、前記受信したデータアクセス対象が第１の認証情報に対して対として格納されている第２の認証情報で認証されるものであるか否かを判定し、

該データアクセス対象が第２の認証情報で認証されるものである場合、第１および第２の認証情報と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可することを特徴とするデータベース制御プログラムを記録した記録媒体。

【請求項１１】　前記アクセスを許可する処理は、前記データ指定情報に対応して該データへのアクセスを許可するアクセス者を指定するアクセス者指定データおよびデータアクセス対象を指定するデータアクセス対象指定データを格納することを特徴とする請求項９または１０記載のデータベース制御プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベースアクセス制御方法およびデータベース装置とデータベース制御プログラムを記録した記録媒体に関し、特に医師のＩＣカードを使用して医療用データベース装置に接続し、患者のＩＣカードを使用して医療用データベース装置に格納されている患者のデータに対してアクセスするデータベースアクセス制御方法およびデータベース装置とデータベース制御プログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】患者のデータを格納した医療用データベースへのアクセスは、従来、医師のＩＣカードのみで認証を行い、この認証結果に基づいてデータベースへのアクセス管理を行っている。

【０００３】すなわち、この種のデータベースは、従来、医師会所属の医師または系列病院の医師のみの使用を目的として構築されているが、今後病診連携や地域医療が進むと、より多くの医師が患者のデータにアクセスする必要が出てきて、同じ患者のデータに対してより多くの医師のアクセスを許す必要が出てくることになるため、患者データの漏洩対策を考慮する必要がある。しかしながら、従来のように医師のＩＣカードのみの認証によるデータアクセス制御では患者データの漏洩時の責任を明確にすることができない。

【０００４】

【発明が解決しようとする課題】上述したように、病診連携や地域医療が進んで、より多くの医師が患者のデータにアクセスし、同じ患者データに対してより多くの医師のアクセスを許すことになると、従来のように医師のＩＣカードのみの認証によるデータアクセス制御では患者データの漏洩時の責任を明確にすることができないという問題があり、医師のＩＣカードの認証結果と患者のＩＣカードの認証結果の両方を用いて、より細かく、安全なデータアクセス制御を行い、患者データの漏洩対策を適確に行う必要がある。

【０００５】本発明は、上記に鑑みてなされたもので、その目的とするところは、例えば医師のようなアクセス者を認証する第１の認証情報と患者のようなデータアクセス対象を認証する第２の認証情報の両認証情報を用いて、データアクセス対象のデータの漏洩を適確に防止し得るデータベースアクセス制御方法およびデータベース装置とデータベース制御プログラムを記録した記録媒体を提供することにある。

【０００６】

【課題を解決するための手段】上記目的を達成するため、請求項１記載の本発明は、端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベースアクセス制御方法であって、端末からアクセス者

を認証する第１の認証情報をデータベース装置に送信し、データベース装置は受信した第１の認証情報を認証して、その認証結果を端末に返送し、端末は受信した認証結果に基づき所望のデータへのアクセスを要求すべく該データを指定するデータ指定情報とともにデータアクセス対象を認証する第２の認証情報をデータベース装置に送信し、データベース装置は受信した第２の認証情報を認証し、この認証結果と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記データ指定情報で指定されるデータへのアクセスを許可することを要旨とする。

【０００７】請求項１記載の本発明にあっては、端末から第１の認証情報をデータベース装置に送信し、データベース装置は第１の認証情報を認証して、認証結果を端末に返送し、端末は認証結果に基づきデータ指定情報とともに第２の認証情報をデータベース装置に送信し、データベース装置は第２の認証情報を認証し、この認証結果とデータ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定するため、本発明を例えば医療データベースに適用した場合、医師の認証情報のみでなく、患者の認証情報によってデータアクセス制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。また、医師の認証情報でデータベースへの接続を行った後は、患者の認証情報のみで患者のデータに次々とアクセスすることができ、業務の流れを妨げずに、患者データへのアクセス制御を円滑に行うことができる。

【０００８】また、請求項２記載の本発明は、端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベースアクセス制御方法であって、端末からアクセス者を認証する第１の認証情報およびデータアクセス対象を認証する第２の認証情報をデータベース装置に送信し、データベース装置は受信した第１の認証情報を認証して、第１の認証情報と第２の認証情報を対にして格納し、端末から所望のデータへのアクセスを要求すべく該データを指定するデータ指定情報とともに第１の認証情報およびデータアクセス対象情報をデータベース装置に送信し、データベース装置は受信した第１の認証情報で前記格納された第１および第２の認証情報の対を参照し、前記受信したデータアクセス対象が第１の認証情報に対して対として格納されている第２の認証情報で認証されるものであるか否かを判定し、該データアクセス対象が第２の認証情報で認証されるものである場合、第１および第２の認証情報と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記データ指定情報で指定されるデータへのアクセスを許可することを要旨とする。

【０００９】請求項２記載の本発明にあっては、端末から第１の認証情報および第２の認証情報をデータベース装置に送信し、データベース装置は第１の認証情報を認証し、第１の認証情報と第２の認証情報を対にして格納し、端末からデータ指定情報とともに第１の認証情報およびデータアクセス対象情報をデータベース装置に送信すると、データベース装置は格納されている第１および第２の認証情報の対を参照し、データアクセス対象が第２の認証情報で認証されるものであるか否かを判定し、そうである場合、第１、第２の認証情報とデータ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定するため、本発明を例えば医療データベースに適用した場合、医師の認証情報のみでなく、患者の認証情報によってデータアクセス制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。また、医師の認証情報が患者の認証情報と対として格納されている医師の場合には患者の認証情報を必要とすることなく、医師の認証情報のみで患者データにアクセスすることができ、これにより患者不在時のデータの入力や参照という主治医に必要な処理を問題なく行なうことができるとともに、また他の病院による診療や投薬の情報も主治医がチェックできるようになる。

【００１０】更に、請求項３記載の本発明は、請求項１または２記載の発明において、前記データ指定情報で指定されるデータへのアクセスの可否を判定する処理が、該データ指定情報に対応して該データへのアクセスを許可するアクセス者を指定するアクセス者指定データおよびデータアクセス対象を指定するデータアクセス対象指定データを格納していることを要旨とする。

【００１１】請求項３記載の本発明にあっては、データ指定情報に対応してアクセス者指定データおよびデータアクセス対象指定データを格納していて、この格納データに基づいてデータへのアクセスの可否を判定するため、本発明を医療データベースに適用した場合には、アクセス者である医師の認証情報のみでなく、データアクセス対象である患者の認証情報によってデータアクセス制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。

【００１２】請求項４記載の本発明は、請求項１または２記載の発明において、前記端末からアクセス者を認証する第１の認証情報をデータベース装置に送信する処理が、ＩＣカードに格納されている第１の認証情報を読み出してデータベース装置に送信し、前記端末からデータアクセス対象を認証する第２の認証情報をデータベース装置に送信する処理が、ＩＣカードに格納されている第２の認証情報を読み出してデータベース装置に送信することを要旨とする。

【００１３】請求項４記載の本発明にあっては、端末ではＩＣカードに格納されている第１の認証情報を読み出してデータベース装置に送信し、ＩＣカードに格納されている第２の認証情報を読み出してデータベース装置に送信する。

【００１４】また、請求項５記載の本発明は、請求項１または２記載の発明において、端末が、前記データ指定情報で指定されるデータへのアクセスを許可された場合、該データ指定情報で指定されるデータに対するデータの変更、追加登録、読み出しを行うことができることを要旨とする。

【００１５】請求項５記載の本発明にあっては、端末はデータへのアクセスを許可された場合、該データに対するデータの変更、追加登録、読み出しを行うことができる。更に、請求項６記載の本発明は、端末からのアクセス者に対して格納しているデータを提供するデータベース装置であって、端末から送信されるアクセス者を認証する第１の認証情報を受信して認証し、この認証結果を端末に返送する認証手段と、端末からデータを指定するデータ指定情報とともに送信されてくるデータアクセス対象を認証する第２の認証情報を受信し、この受信した第２の認証情報を認証し、この認証結果と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可するアクセス許可手段とを有することを要旨とする。

【００１６】請求項６記載の本発明にあっては、端末から第１の認証情報をデータベース装置に送信し、データベース装置は第１の認証情報を認証して、認証結果を端末に返送し、端末は認証結果に基づきデータ指定情報とともに第２の認証情報をデータベース装置に送信し、データベース装置は第２の認証情報を認証し、この認証結果とデータ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定するため、本発明を例えば医療データベースに適用した場合、医師の認証情報のみでなく、患者の認証情報によってデータアクセス制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。また、医師の認証情報でデータベースへの接続を行った後は、患者の認証情報のみで患者のデータに次々とアクセスすることができ、業務の流れを妨げずに、患者データへのアクセス制御を円滑に行うことができる。

【００１７】請求項７記載の本発明は、端末からのアクセス者に対して格納しているデータを提供するデータベース装置であって、端末から送信されるアクセス者を認証する第１の認証情報およびデータアクセス対象を認証する第２の認証情報を受信し、この受信した第１の認証情報を認証し、第１の認証情報と第２の認証情報を対にして格納する格納手段と、端末からデータを指定するデータ指定情報とともに送信されてくる第１の認証情報およびデータアクセス対象情報を受信し、この受信した第１の認証情報で前記格納手段に格納されている第１および第２の認証情報の対を参照し、前記受信したデータアクセス対象が第１の認証情報に対して対として格納されている第２の認証情報で認証されるものであるか否かを判定し、該データアクセス対象が第２の認証情報で認証されるものである場合、第１および第２の認証情報と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可するアクセス許可手段とを有することを要旨とする。

【００１８】請求項７記載の本発明にあっては、端末から第１の認証情報および第２の認証情報をデータベース装置に送信し、データベース装置は第１の認証情報を認証し、第１の認証情報と第２の認証情報を対にして格納し、端末からデータ指定情報とともに第１の認証情報およびデータアクセス対象情報をデータベース装置に送信すると、データベース装置は格納されている第１および第２の認証情報の対を参照し、データアクセス対象が第２の認証情報で認証されるものであるか否かを判定し、そうである場合、第１、第２の認証情報とデータ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定するため、本発明を例えば医療データベースに適用した場合、医師の認証情報のみでなく、患者の認証情報によってデータアクセス制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。また、医師の認証情報が患者の認証情報と対として格納されている医師の場合には患者の認証情報を必要とすることなく、医師の認証情報のみで患者データにアクセスすることができ、これにより患者不在時のデータの入力や参照という主治医に必要な処理を問題なく行なうことができるとともに、また他の病院による診療や投薬の情報も主治医がチェックできるようになる。

【００１９】また、請求項８記載の本発明は、請求項６または７記載の発明において、前記アクセス許可手段が、前記データ指定情報に対応して該データへのアクセスを許可するアクセス者を指定するアクセス者指定データおよびデータアクセス対象を指定するデータアクセス対象指定データを蓄積する蓄積手段を有することを要旨とする。

【００２０】請求項８記載の本発明にあっては、データ指定情報に対応してアクセス者指定データおよびデータアクセス対象指定データを格納していて、この格納データに基づいてデータへのアクセスの可否を判定するため、本発明を医療データベースに適用した場合には、アクセス者である医師の認証情報のみでなく、データアクセス対象である患者の認証情報によってデータアクセス

制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。

【００２１】更に、請求項９記載の本発明は、端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベース制御プログラムを記録した記録媒体であって、端末から送信されるアクセス者を認証する第１の認証情報を受信して認証し、この認証結果を端末に返送し、端末からデータを指定するデータ指定情報とともに送信されてくるデータアクセス対象を認証する第２の認証情報を受信し、この受信した第２の認証情報を認証し、この認証結果と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可するデータベース制御プログラムを記録媒体に記録することを要旨とする。

【００２２】請求項９記載の本発明にあっては、端末から第１の認証情報をデータベース装置に送信し、データベース装置は第１の認証情報を認証して、認証結果を端末に返送し、端末は認証結果に基づきデータ指定情報とともに第２の認証情報をデータベース装置に送信し、データベース装置は第２の認証情報を認証し、この認証結果とデータ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定するデータベース制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００２３】請求項１０記載の本発明は、端末からデータベース装置にアクセスしたアクセス者に対してデータベース装置に格納されているデータへのアクセスを制御するデータベース制御プログラムを記録した記録媒体であって、端末から送信されるアクセス者を認証する第１の認証情報およびデータアクセス対象を認証する第２の認証情報を受信し、この受信した第１の認証情報を認証し、第１の認証情報と第２の認証情報を対にして格納し、端末からデータを指定するデータ指定情報とともに送信されてくる第１の認証情報およびデータアクセス対象情報を受信し、この受信した第１の認証情報で前記格納されている第１および第２の認証情報の対を参照し、前記受信したデータアクセス対象が第１の認証情報に対して対として格納されている第２の認証情報で認証されるものであるか否かを判定し、該データアクセス対象が第２の認証情報で認証されるものである場合、第１および第２の認証情報と前記データ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定し、アクセス可である場合、前記指定用データで指定されるデータへのアクセスを許可するデータベース制御プログラムを記録媒体に記録することを要旨とする。

【００２４】請求項１０記載の本発明にあっては、端末から第１の認証情報および第２の認証情報をデータベース装置に送信し、データベース装置は第１の認証情報を認証し、第１の認証情報と第２の認証情報を対にして格納し、端末からデータ指定情報とともに第１の認証情報およびデータアクセス対象情報をデータベース装置に送信すると、データベース装置は格納されている第１および第２の認証情報の対を参照し、データアクセス対象が第２の認証情報で認証されるものであるか否かを判定し、そうである場合、第１、第２の認証情報とデータ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定するデータベース制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００２５】また、請求項１１記載の本発明は、請求項９または１０記載の発明において、前記アクセスを許可する処理が、前記データ指定情報に対応して該データへのアクセスを許可するアクセス者を指定するアクセス者指定データおよびデータアクセス対象を指定するデータアクセス対象指定データを格納するデータベース制御プログラムを記録媒体に記録することを要旨とする。

【００２６】請求項１１記載の本発明にあっては、データ指定情報に対応してアクセス者指定データおよびデータアクセス対象指定データを格納していて、この格納データに基づいてデータへのアクセスの可否を判定するデータベース制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００２７】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。図１は、本発明の一実施形態に係るデータベースアクセス制御方法を実施するＩＣカードを用いたデータベースアクセス制御システムの構成を示すブロック図である。同図に示すデータベースアクセス制御システムは、一例として医療用データベースシステムを構成するものであり、本データベースへのアクセス者である医師によって操作される利用者端末１および該利用者端末１に通信回線５を介して接続されているデータベースシステム７を有する。通信回線５は、例えばＬＡＮ回線、ＩＳＤＮ回線、アナログ回線、光ケーブル回線などのような種々の通信回線で構成され得るものである。

【００２８】利用者端末１は、ＩＣカードリーダ３を有し、このＩＣカードリーダ３に利用者である医師の認証情報などが記憶された医師用のＩＣカードや患者の認証情報などが記憶された患者用のＩＣカードを挿入すると、これらのＩＣカードに記憶された認証情報などの情報はＩＣカードリーダ３で読み取られて、利用者端末１に入力されるようになっている。そして、利用者端末１は、ＩＣカードリーダ３から読み込んだ認証情報などの情報を通信回線５を介してデータベースシステム７に送

信し得るようになっている。また、利用者端末１は、データベースシステム７から送信されるデータを通信回線５を介して受信し、利用者が視覚的に認識し得るように表示する機能を有している。

【００２９】データベースシステム７は、通信回線５を介して利用者端末１に接続され、利用者端末１とデータの送受信を行う通信モジュール９、認証処理を行う認証モジュール１１、データアクセス制御を行うデータアクセス制御モジュール１３、データアクセス管理情報を格納するアクセス管理データベース１５、およびデータを格納するデータベース１７から構成されている。

【００３０】更に詳しくは、通信モジュール９は利用者端末１から受信したデータを認証モジュール１１やデータアクセス制御モジュール１３へ送信する機能、認証モジュール１１やデータアクセス制御モジュール１３より受信したデータを利用者端末１へ送信する機能、利用者端末１とデータベースシステム７との接続を行う機能を有する。認証モジュール１１は通信モジュール９よりＩＣカードデータを受信する機能、ＩＣカードデータより認証を行う機能、認証結果を通信モジュール９へ送信する機能を有する。

【００３１】データアクセス制御モジュール１３はアクセス管理データベース１５、データベース１７と接続されており、通信モジュール９より認証結果やアクセスしたいデータを指定するデータを受信する機能、それらをアクセス管理データベース１５と照合する機能、照合結果によってデータベース１７よりデータを通信モジュール９へ送信する機能を有する。

【００３２】なお、本実施形態では、認証モジュール１１をデータベースシステム７がその一部として有するような構成となっているが、認証モジュール１１をデータベースシステム７とは別に例えば認証サーバとして設けてもよいものである。

【００３３】図２（ａ），（ｂ）は、アクセス管理データベース１５に格納されているデータ管理テーブルの構成を示す図である。図２（ａ）に示すデータ管理テーブルは、データ毎にアクセスの可能な患者と医師を管理するテーブルであり、データを指定するデータ、すなわちデータ指定情報に対応して、患者を指定するデータおよび医師を指定するデータが登録されている。また、図２（ｂ）に示すデータ管理テーブルは、患者毎にアクセス可能な医師を管理するテーブルであり、患者を指定するデータに対応して医師を指定するデータが登録されている。

【００３４】次に、図３～図８に示すフローチャートを参照して、以上のように構成されるデータベースアクセス制御システムの作用について説明する。なお、この説明における前提条件として、ＩＣカードとは、医師、患者が１人１枚以上持っており、ＩＣカードには認証モジュール１１で認証するのに十分であるデータが蓄積されているものとし、また、医師が特定の目的のためだけにデータにアクセスし、患者データの漏洩を防止するために、患者のデータに医師がアクセスする際には、医師のＩＣカードと患者のＩＣカードを必須とすることを前提にする。

【００３５】まず、図３に示すフローチャートを参照して、医師が利用者端末１を通信回線５を介してデータベースシステム７に接続する方法について説明する。この方法は医師の認証データを通信モジュール９に送信する機能と、医師認証データにより認証を行う機能とに分けられる。

【００３６】まず、医師の認証データを通信モジュール９に送信する機能を説明する。医師は利用者端末１でデータベースシステム７へ接続要求を送信する（ステップＳ１１）。通信モジュール９は利用者端末１へ医師認証データ要求を送信する（ステップＳ１３）。利用者端末１は通信モジュール９からの医師認証データ要求を受信して、ディスプレイ上に医師のＩＣカード挿入を促すメッセージを表示する。医師がＩＣカードをＩＣカードリーダに挿入すると（ステップＳ１５）、ＩＣカード内の認証データが通信モジュール９へ送信される（ステップＳ１７）。通信モジュール９への送信は自動的に行っても、医師にボタンなどをクリックさせてもどちらでも構わない。

【００３７】医師認証データにより認証を行う機能を説明する。通信モジュール９は利用者端末１から受信した認証データを認証モジュール１１に送信する（ステップＳ１９）。認証モジュール１１は受信した認証データで認証を行う（ステップＳ２１）。認証結果を通信モジュール９に送信する（ステップＳ２３）。認証結果を判定し（ステップＳ２５）、認証が正しく行われていなければ、通信モジュール９は利用者端末１に接続不可メッセージを送信する（ステップＳ２７）。利用者端末１は接続不可メッセージを受信し、接続ができなかったことをディスプレイに表示し、ＩＣカードを返却する（ステップＳ２９）。認証が正しく行われていれば、通信モジュール９は利用者端末１とデータベースシステム７との接続を行う（ステップＳ３１）。

【００３８】利用者端末１がデータベースシステム７に接続されると、医師は利用者端末１からデータベースシステム７に対して新しいデータの入力、既存のデータへのアクセス、主治医の登録または本処理の終了のいずれかを行うことになる（ステップＳ３３）。新しいデータの入力を行う場合には、飛び越し記号Ｂを介して図４に示す処理に移行し、また既存のデータへのアクセスを行う場合には、飛び越し記号Ｃを介して図５に示す処理に移行し、主治医の登録を行う場合には、飛び越し記号Ｅを介して図６に示す処理に移行することになる。

【００３９】次に、まず図４に示すフローチャートを参照して、新しいデータの入力、すなわち患者ＩＣカード

の認証を行って、新しい患者データの登録を行う方法について説明する。この方法は患者の認証データを通信モジュールに送信する機能、認証データにより認証を行う機能、認証結果を利用者端末に送信する機能、利用者端末から登録データを送信する機能、データにアクセスさせるためのアクセス管理データを登録する機能、データベースにデータを登録する機能とに分けられる。

【００４０】まず、患者の認証データを通信モジュール９に送信する機能を説明する。この場合には、最初に患者のＩＣカードを使用するか否かがチェックされる（ステップＳ４１）。患者のＩＣカードを使用しない場合には、飛び越し記号Ｄを介して図７および図８に示す処理に移行するが、ここでは患者のＩＣカードを使用する場合について説明する。

【００４１】医師は、利用者端末１のディスプレイ上で新しい患者のデータを登録する作業を行うことを指定する。ディスプレイ上で患者ＩＣカードを使用してデータの登録を行う作業を行うことを指定すると、患者のＩＣカード挿入を促すメッセージを表示する。患者ＩＣカードをＩＣカードリーダに挿入すると（ステップＳ４３）、ＩＣカード内の認証データが通信モジュールへ送信される（ステップＳ４５）。通信モジュール９への送信は自動的に行っても、医師や患者にボタンなどをクリックさせてもどちらでも構わない。

【００４２】患者認証データにより認証を行う機能を説明する。通信モジュール９は利用者端末１から受信した認証データを認証モジュール１１に送信する（ステップＳ４７）。認証モジュール１１は受信した認証データで認証を行う（ステップＳ４９）。

【００４３】次に、認証結果を利用者端末１に送信する機能を説明する。認証モジュール１１は認証結果を通信モジュール９に送信する。通信モジュール９は認証結果を判定し（ステップＳ５３）、認証が正しく行われていなければ、通信モジュール９は利用者端末１に登録不可メッセージを送信する（ステップＳ５５）。利用者端末１は登録不可メッセージを受信し、登録できないことをディスプレイに表示し、患者ＩＣカードを返却する（ステップＳ５７）。そして、処理は図３のステップＳ３３に戻る。

【００４４】利用者端末１から登録データを送信する機能を説明する。患者認証が正しく行われれば、利用者端末１から認証した患者に関する登録データを通信モジュール９に送信する（ステップＳ５９）。通信モジュール９に送信される登録データはアクセス管理データベース１５に登録するデータと、データベース１７に登録するデータである。

【００４５】データにアクセスさせるためのアクセス管理データを登録する機能を説明する。通信モジュール９はアクセス管理データベース１５に登録するデータを送信する（ステップＳ６１）。アクセス管理データベース１５に登録するデータの概念は図２（ａ）で示すものである。データベース１７に登録するデータを指定するデータと一緒に認証した患者を指定するデータと認証した医師を指定するデータをアクセス管理データベース１５に登録する（ステップＳ６３）。データベース１７に蓄積するデータへのアクセスはここで登録した患者と医師の認証が必須になる。診療上、他の医師にもこのデータへのアクセスを許す必要があれば、同じデータを指定するデータと患者を指定するデータにおいて、他の医師を指定するデータを登録しても構わない。

【００４６】データベース１７にデータを登録する機能を説明する。利用者端末１から受信したデータをデータベース１７に登録する（ステップＳ６５）。登録が終了したら、図３のステップＳ３３に戻り、医師の認証完了時の状態に戻る。

【００４７】次に、図５に示すフローチャートを参照して、既存のデータへのアクセス、すなわち患者ＩＣカードを使用して、患者データへアクセスする方法を説明する。この方法はアクセスしたいデータを指定する機能、患者の認証データを通信モジュール９に送信する機能、患者認証データにより認証を行う機能、データアクセス制御を行う機能とに分けられる。

【００４８】まず、アクセスしたいデータを指定する機能を説明する。利用者端末１とデータベースシステム７とが接続されたら（ステップＳ３１）、医師認証結果よりアクセス管理データベースを検索する（ステップＳ７１）。これは図２（ａ）で医師を指定するデータと一致するデータを検索するということである。検索した結果を基に、データベース１７にて当該医師にアクセスを許すリストを作成し、アクセス可能データリストを通信モジュールへ送信する（ステップＳ７３）。通信モジュール９は受信したアクセス可能データリストを利用者端末１へ送信する（ステップＳ７５）。利用者端末１はアクセス可能データリストを表示する（ステップＳ７７）。このアクセスを許すリストはデータを指定するデータより作成されたデータの一覧であるが、データを選択しやすいように患者でソートするなどの工夫がしてあっても構わない。

【００４９】医師がアクセスしたいデータがなければステップＳ３３に戻って、医師の認証完了時の状態に戻る（ステップＳ７７のＮＯ）。医師がアクセスしたいデータがあれば、そのデータをクリックして通信モジュール９へアクセスしたいデータを指定するデータを送信する（ステップＳ８１）。

【００５０】次に、患者の認証データを通信モジュール９に送信する機能を説明する。通信モジュール９はアクセスしたいデータを指定するデータを受信後、患者認証データ要求を利用者端末１に送信する（ステップＳ８３）。利用者端末１は患者認証データ要求を通信モジュールより受信して、ディスプレイ上に患者ＩＣカード挿

入を促すメッセージを表示する。医師は、医師ＩＣカードを取り出し、患者ＩＣカードをＩＣカードリーダ３に挿入する（ステップＳ８５）。患者認証データを通信モジュール９に送信する（ステップＳ８７）。通信モジュール９への患者認証データの送信は自動的に行っても医師によるボタンのクリックなどで行ってもどちらでも構わない。

【００５１】患者認証データにより認証を行う機能を説明する。通信モジュール９は利用者端末１より受信した患者認証データを認証モジュール１１へ送信する（ステップＳ８９）。認証モジュール１１は受信した認証データで認証を行う（ステップＳ９１）。認証結果を通信モジュールに送信する（ステップＳ９３）。通信モジュール９は、認証結果を判定し（ステップＳ９５）、認証が正しく行われていなければ、通信モジュール９は利用者端末１にアクセス不可メッセージを送信する（ステップＳ９７）。利用者端末１はアクセス不可メッセージを受信し（ステップＳ９９）、データにアクセスができなかったことをディスプレイに表示し、ＩＣカードを返却する。ＩＣカード返却後、ステップＳ７７に戻り、当該医師がアクセス可能なアクセス可能データリストを表示し、以下同様の処理を行う。

【００５２】認証が正しく行われていれば、通信モジュール９はデータアクセス制御モジュール１３にアクセスしたいデータを指定するデータと医師認証結果、患者認証結果を送信する。

【００５３】次に、データアクセス制御を行う機能を説明する。アクセス管理データベース１５により医師認証結果、患者認証結果が指定されたデータへのアクセス条件として十分であるかどうかの照合を行う（ステップＳ１０１）。これは図２（ａ）でデータを指定したデータと一致するデータを検索した時、患者を指定するデータと医師を指定するデータがそれぞれの認証結果と一致するかどうか照合するということである。照合の結果、アクセス不可であれば、アクセス管理データベース１５は通信モジュール９へアクセス不可メッセージを送信する。通信モジュール９は利用者端末１にアクセス不可メッセージを送信する（ステップＳ９７）。利用者端末１はアクセス不可メッセージを受信し、データにアクセスができなかったことをディスプレイに表示し、ＩＣカードを返却する。ＩＣカード返却後、ステップＳ７７に戻り、当該医師がアクセス可能なアクセス可能データリストを表示し、以下同様の処理を行う。

【００５４】照合の結果、アクセス可能であれば、アクセス管理データベース１５はデータベース１７へ当該データを通信モジュール９へ送信するように要求をかける。データベース１７は当該データを通信モジュール９へ送信する（ステップＳ１０３）。通信モジュール９は当該データを利用者端末１へ送信する（ステップＳ１０５）。利用者端末１は受信した当該患者データをディスプレイに表示する（ステップＳ１０７）。患者データを使用して作業を行った後には当該患者データの表示を終了し、ステップＳ７７に戻り、医師がアクセス可能データリストを表示する。

【００５５】上述した説明では、医師が特定の目的のためだけにデータにアクセスし、患者データの漏洩を防止するために、患者のデータに医師がアクセスする際には、医師のＩＣカードと患者のＩＣカードを必須とすることを前提にした。しかし、実際の医療業務では、主治医は患者帰宅後に患者データへのアクセスを行うことが求められ、患者ＩＣカードが無いために患者のデータへのアクセスができないという問題が生じる。また、他院により入力された患者のデータに主治医であるにもかかわらずアクセスできないという問題が生じる。その問題を解決するためには、患者のＩＣカードを必須としないデータの登録やアクセスを可能にするという前提に基づいた方式が必要である。しかし、どの医師に対しても無条件に患者データへのアクセスを許すのでは患者データ漏洩時の責任の明確化ができない。そのために、患者が主治医と指定した医師のみに患者のデータを患者ＩＣカード無しでも登録したりアクセスしたりできるようにする処理について図６を参照して説明する。

【００５６】図６に示すフローチャートを参照して、主治医を登録する処理、すなわち患者ＩＣカードの認証を行って、患者に主治医を登録する方法を説明する。なお、この方法では、図３に示した医師の認証結果を基にして利用者端末１とデータベースシステム７との接続を行うまでの処理は図３に示す処理と同じである。また、この方法は患者の認証データを通信モジュール９に送信する機能、認証データにより認証を行う機能、認証結果を利用者端末１に送信する機能、利用者端末１から登録する患者の主治医データを送信する機能、アクセス管理データベースに患者の主治医を登録する機能とに分けられる。

【００５７】まず、患者の認証データを通信モジュール９に送信する機能を説明する。ディスプレイ上で患者に主治医を登録する作業を行うことを指定する。患者のＩＣカード挿入を促すメッセージを表示する。患者ＩＣカードをＩＣカードリーダ３に挿入すると（ステップＳ１１１）、ＩＣカード内の認証データが通信モジュールへ送信される（ステップＳ１１３）。通信モジュール９への送信は自動的に行っても、医師や患者にボタンなどをクリックさせてもどちらでも構わない。

【００５８】患者認証データにより認証を行う機能を説明する。通信モジュール９は利用者端末１から受信した認証データを認証モジュール１１に送信する（ステップＳ１５）。認証モジュール１１は受信した認証データで認証を行う（ステップＳ１１７）。

【００５９】認証結果を利用者端末１に送信する機能を説明する。認証モジュール１１は認証結果を通信モジュ

ール9に送信する（ステップS119）。通信モジュール9は、認証結果を判定し（ステップS121）、認証が正しく行われていなければ、通信モジュール9は利用者端末1に登録不可メッセージを送信する（ステップS123）。利用者端末1は登録不可メッセージを受信し（ステップS125）、登録できないことをディスプレイに表示し、患者ICカードを返却する。そして、ステップS33に戻る。

【0060】利用者端末1から登録する患者の主治医データを送信する機能を説明する。患者認証が正しく行われれば、利用者端末1からデータベースシステム7に接続した医師を認証した患者の主治医として登録する登録データを通信モジュール9に送信する（ステップS127）。

【0061】アクセス管理データベースに患者の主治医を登録する機能を説明する。通信モジュール9はアクセス管理データベース15に登録するデータを送信する（ステップS129）。アクセス管理データベース15に登録するデータの概念は図2（b）で示すものであり、患者を指定するデータについて、患者が主治医として認めた医師を指定するデータを登録する（ステップS131）。データ登録後、ステップS33に戻り、医師の認証完了時の状態に戻る。

【0062】次に、図7に示すフローチャートを参照して、患者のICカードを使用しないで、医師の主治医の権限で新しい患者データを登録する方法について説明する。この方法は利用者端末1から登録データを送信する機能、アクセス管理データベース15で認証された医師が患者データの主治医であるかのチェックを行う機能、登録するデータにアクセスさせるためのアクセス管理データを登録する機能、データベース17にデータを登録する機能とに分けられる。

【0063】まず、利用者端末1から登録データを送信する機能を説明する。利用者端末1からデータベース17に登録したいデータとそのデータへのアクセス管理のためのデータを通信モジュール9に送信する（ステップS141）。通信モジュール9は利用者端末1から受信したデータをアクセス管理データベース15へ送信する（ステップS143）。

【0064】アクセス管理データベース15で認証された医師が患者データの主治医であるかのチェックを行う機能を説明する。アクセス管理データベース15を検索することにより、登録しようとしている患者の主治医が認証された医師であるかどうか照合を行う（ステップS145）。これは図2（b）で登録しようとしている患者を指定するデータに対して認証された医師を指定するデータが登録されているか否かについての検索を行うことである。照合の結果、医師が患者の主治医として登録されていなければ通信モジュールに登録不可メッセージを送信する。通信モジュール9は登録不可メッセージを利用者端末1に送信する（ステップS147）。利用者端末1は登録不可メッセージを受信し、登録できないことをディスプレイに表示し（ステップS149）、医師の認証完了時の状態であるステップS33に戻る。

【0065】次に、登録するデータにアクセスさせるためのアクセス管理データを登録する機能を説明する。アクセス管理データベース15に登録するデータの概念は図2（a）で示すものであり、データベース17に登録するデータを指定するデータと一緒に患者を指定するデータと認証した医師を指定するデータをアクセス管理データベース15に登録する（ステップS151）。データベース17に蓄積するデータへのアクセスはここで登録した患者と医師の認証は必須になる。診療上、他の医師にもこのデータへのアクセスを許す必要があれば、同じデータを指定するデータと患者を指定するデータにおいて、他の医師を指定するデータを登録しても構わない。

【0066】データベース17にデータを登録する機能を説明する。利用者端末1から受信したデータをデータベース17に登録する（ステップS153）。登録が終了したら、医師の認証完了時の状態であるステップS33に戻る。

【0067】次に、図8に示すフローチャートを参照して、患者のICカードを使用しないで、医師の主治医の権限で患者データにアクセスする方法について説明する。この方法は、利用者端末1から患者を指定するデータを送信する機能、アクセス管理データベース15で認証された医師が患者の主治医であるかのチェックを行う機能、アクセス可能データリストを利用者端末1に送信する機能、利用者端末1からアクセスしたいデータを指定するデータを送信する機能、データベース17が利用者端末1へデータを送信する機能とに分けられる。

【0068】まず、利用者端末1から患者を指定するデータを送信する機能を説明する。患者を指定したデータの参照を行うか否かの判定を行い（ステップS161）、参照しない場合は、ここで医師の認証完了時の状態であるステップS33に戻る。患者を指定したデータの参照を行う場合は、患者を指定するデータと医師の認証結果をアクセス管理データベース15に送信する（ステップS163）。

【0069】次に、アクセス管理データベース15で認証された医師が患者の主治医であるかのチェックを行う機能を説明する。アクセス管理データベース15を検索することにより、指定した患者の主治医が認証された医師であるかどうか照合を行う（ステップS165）。これは図2（b）で指定された患者を指定するデータに対して認証された医師を指定するデータが登録されているか検索を行うことである。照合の結果、医師が患者の主治医として登録されていなければ通信モジュール9にアクセス不可メッセージを送信する。通信モジュール9は

アクセス不可メッセージを利用者端末１に送信する（ステップＳ１６７）。利用者端末１はアクセス不可メッセージを受信し（ステップＳ１６９）、アクセスできないことをディスプレイに表示し、医師の認証完了時の状態であるステップＳ３３に戻る。

【００７０】アクセス可能データリストを利用者端末１に送信する機能を説明する。患者に対して医師が主治医として登録されていれば、患者を指定するデータによりデータベース１７を検索する。これは、図２（ａ）で患者を指定するデータと一致するデータを検索して、データベース１７よりリストを作成してもいいし、直接データベース１７を患者を指定するデータで検索しても構わない。検索した結果を基に、データベース１７にて当該医師にアクセスを許すリストを作成し、アクセス可能データリストを通信モジュール９へ送信する（ステップＳ１７１）。通信モジュール９は受信したアクセス可能データリストを利用者端末１へ送信する（ステップＳ１７３）。

【００７１】利用者端末１からアクセスしたいデータを指定するデータを送信する機能を説明する。利用者端末１はアクセス可能データリストを表示する（ステップＳ１７５）。医師がアクセスしたいデータがなければ、医師の認証完了時の状態であるステップＳ３３に戻る。医師がアクセスしたいデータがあれば、そのデータをクリックして送信する（ステップＳ１７７，Ｓ１７９）。

【００７２】データベース１７が利用者端末１へデータを送信する機能を説明する。データベース１７は利用者端末１より受信したアクセスしたいデータを指定するデータによりデータベース１７を検索し、当該データを通信モジュール９へ送信する（ステップＳ１８１）。通信モジュール９はデータベース１７より受信したデータを利用者端末１へ送信する（ステップＳ１８３）。利用者端末１は受信したデータをディスプレイに表示する（ステップＳ１８５）。患者データを使用して作業を行った後には当該患者データの表示を終了し、ステップＳ１７５に戻って、医師がアクセス可能データリストを表示する。

【００７３】なお、上記実施形態のデータベースアクセス制御方法の処理手順をプログラムとして記録媒体に記録して、この記録媒体をコンピュータシステムに組み込むとともに、該記録媒体に記録されたプログラムをコンピュータシステムにダウンロードまたはインストールし、該プログラムでコンピュータシステムを作動させることにより、データベースアクセス制御方法を実施するデータベースアクセス制御システムとして機能させることができることは勿論であり、このような記録媒体を用いることにより、その流通性を高めることができるものである。

【００７４】

【発明の効果】以上説明したように、本発明によれば、端末から第１の認証情報をデータベース装置に送信し、データベース装置は第１の認証情報を認証して認証結果を端末に返送し、端末は認証結果に基づきデータ指定情報とともに第２の認証情報をデータベース装置に送信し、データベース装置は第２の認証情報を認証し、この認証結果とデータ指定情報に基づき該データ指定情報で指定されるデータへのアクセスの可否を判定するので、本発明を例えば医療データベースに適用した場合、医師の認証情報のみでなく、患者の認証情報によってデータアクセス制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。また、医師の認証情報でデータベースへの接続を行った後は、患者の認証情報のみで患者のデータに次々とアクセスすることができ、業務の流れを妨げずに、患者データへのアクセス制御を円滑に行うことができる。更に、患者毎にアクセス可能な医師を管理することにより、例えば患者が主治医と見なした医師のみに対して他の医療設備などによって入力された患者データへのアクセス、患者不在時の患者データへのアクセスを可能にすることができ、これにより患者不在時のデータの入力や参照という主治医に必要な処理を問題なく行うことができるとともに、また他の病院による診療や投薬の情報も主治医がチェックできるようになる。

【００７５】また、本発明によれば、端末から第１および第２の認証情報をデータベース装置に送信し、データベース装置は第１の認証情報を認証して、第１および第２の認証情報を対にして格納し、端末からデータ指定情報とともに第１の認証情報およびデータアクセス対象情報をデータベース装置に送信すると、データベース装置は第１および第２の認証情報の対を参照し、データアクセス対象が第２の認証情報で認証されるものである場合、データ指定情報で指定されるデータへのアクセスの可否を判定するので、本発明を例えば医療データベースに適用した場合、医師の認証情報のみでなく、患者の認証情報によってデータアクセス制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。また、医師の認証情報が患者の認証情報と対として格納されている医師の場合には患者の認証情報を必要とすることなく、医師の認証情報のみで患者データにアクセスすることができ、症例検索など医療の質の向上のために患者データを有効活用することができる。更に、患者毎にアクセス可能な医師を管理することにより、例えば患者が主治医と見なした医師のみに対して他の医療設備などによって入力された患者データへのアクセス、患者不在時の患者データへのアクセスを可能にすることができ、これにより患者不在時のデータの入力や参照という主治医に必要な処理を問題なく行うことができるとともに、また他の病院により診療や投薬の情報も主治医がチェックで

きるようになる。

【００７６】更に、本発明によれば、データ指定情報に対応してアクセス者指定データおよびデータアクセス対象指定データを格納していて、この格納データに基づいてデータへのアクセスの可否を判定するため、本発明を医療データベースに適用した場合には、アクセス者である医師の認証情報のみでなく、データアクセス対象である患者の認証情報によってデータアクセス制御をデータ毎に行うことができ、医師による患者データの目的外使用および患者データの漏洩を適確に防止することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るデータベースアクセス制御方法を実施するＩＣカードを用いたデータベースアクセス制御システムの構成を示すブロック図である。

【図２】図１に示す実施形態に使用されているアクセス管理データベースに格納されているデータ管理テーブルの構成を示す図である。

【図３】図１に示す実施形態において医師が利用者端末を通信回線を介してデータベースシステムに接続する方法を示すフローチャートである。

【図４】図１に示す実施形態において患者ＩＣカードの認証を行って、新しい患者データの登録を行う方法を示すフローチャートである。

【図５】図１に示す実施形態において患者ＩＣカードを使用して、患者データへアクセスする方法を示すフローチャートである。

【図６】図１に示す実施形態において患者ＩＣカードの認証を行って、患者に主治医を登録する方法を示すフローチャートである。

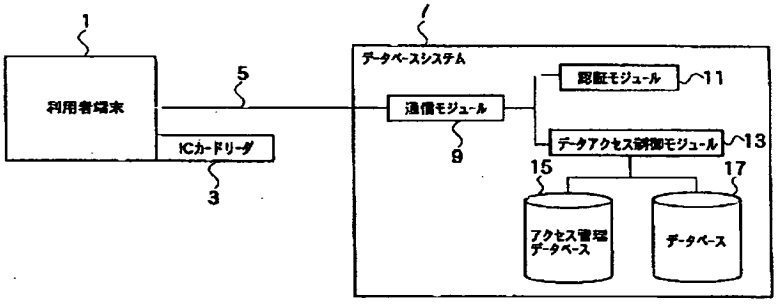
【図７】図１に示す実施形態において患者のＩＣカードを使用しないで、医師の主治医の権限で新しい患者データを登録する方法を示すフローチャートである。

【図８】図１に示す実施形態において患者のＩＣカードを使用しないで、医師の主治医の権限で患者データをアクセスする方法を示すフローチャートである。

【符号の説明】

１　利用者端末
３　ＩＣカードリーダ
５　通信回線
７　データベースシステム
９　通信モジュール
１１　認証モジュール
１３　データアクセス制御モジュール
１５　アクセス管理データベース
１７　データベース

【図１】



【図2】

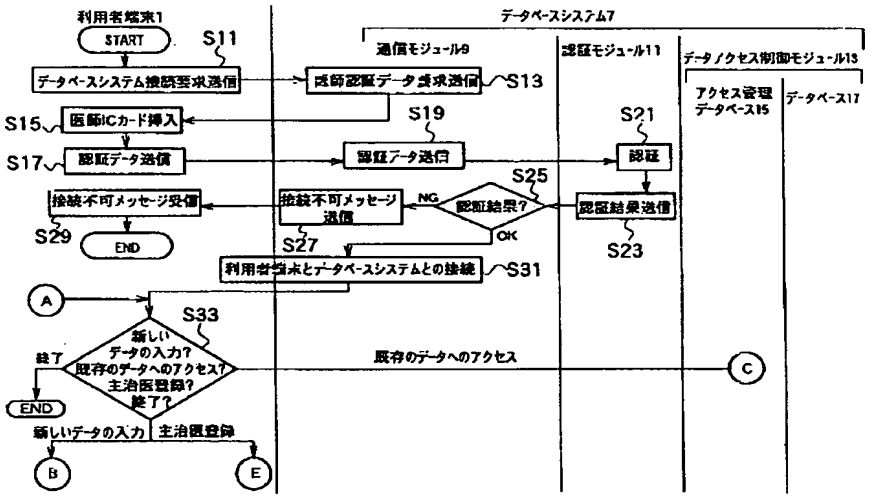
(a)

データを指定するデータ	患者を指定するデータ	医師を指定するデータ

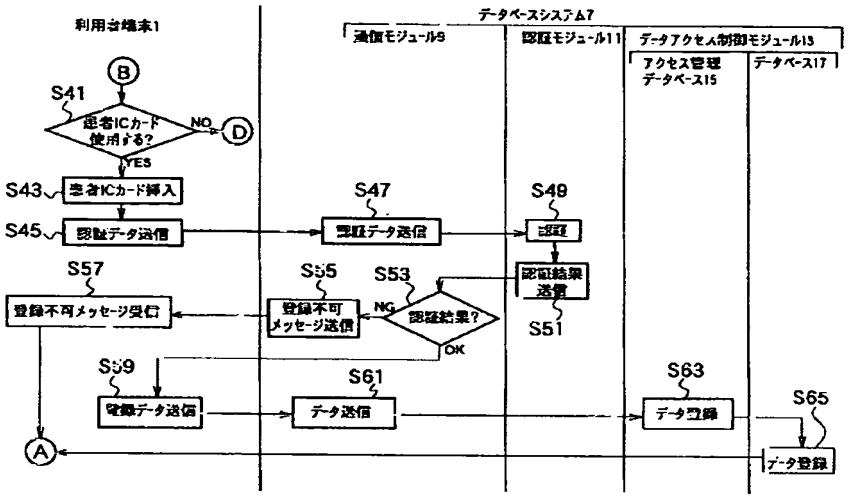
(b)

患者を指定するデータ	医師を指定するデータ

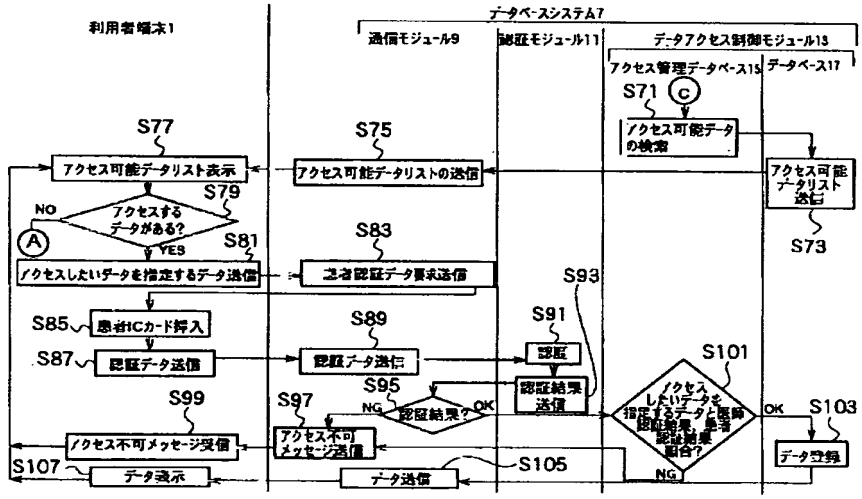
【図3】



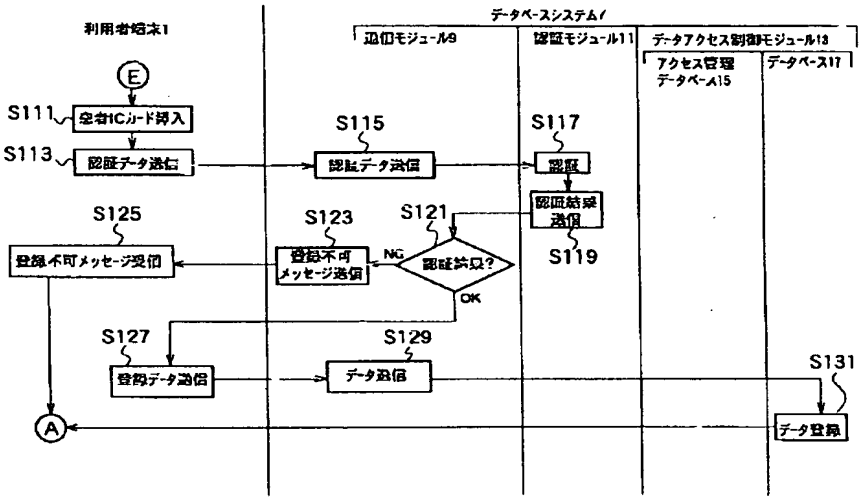
【図4】


利用者端末1
データベースシステム7
通信モジュール9
認証モジュール11
データアクセス制御モジュール13
アクセス管理データベース15
データベース17
S41
患者ICカード使用する?
NO
YES
S43
患者ICカード挿入
S45
認証データ送信
S47
認証データ送信
S49
認証
S51
認証結果送信
S53
認証結果?
NG
OK
S55
登録不可メッセージ送信
S57
登録不可メッセージ受信
S59
登録データ送信
S61
データ送信
S63
データ登録
S65
データ登録

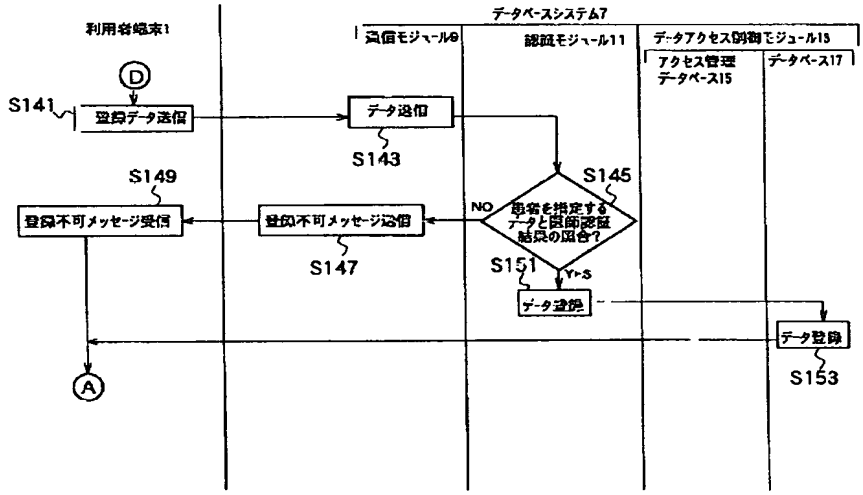
【図5】


利用者端末1
データベースシステム7
通信モジュール9
認証モジュール11
データアクセス制御モジュール13
アクセス管理データベース15
データベース17
S71
アクセス可能データの検索
S73
アクセス可能データリスト送信
S75
アクセス可能データリストの送信
S77
アクセス可能データリスト表示
S79
アクセスするデータがある?
NO
YES
S81
アクセスしたいデータを指定するデータ送信
S83
患者認証データ要求送信
S85
患者ICカード挿入
S87
認証データ送信
S89
認証データ送信
S91
認証
S93
認証結果送信
S95
認証結果?
NG
OK
S97
アクセス不可メッセージ送信
S99
アクセス不可メッセージ受信
S101
アクセスしたいデータを指定するデータと医師認証結果、患者認証結果照合?
OK
NG
S103
データ登録
S105
データ送信
S107
データ表示

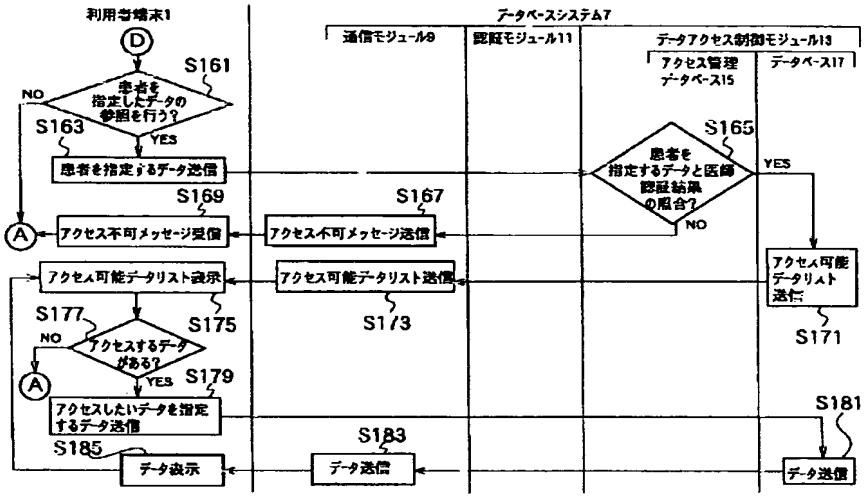
【図6】


利用者端末1
データベースシステム7
通信モジュール9
認証モジュール11
データアクセス制御モジュール13
アクセス管理データベース15
データベース17
E
S111
S113
S115
S117
S119
S121
S123
S125
S127
S129
S131
A
NG
OK
認証結果?
データ登録

【図7】


利用者端末1
データベースシステム7
通信モジュール9
認証モジュール11
データアクセス制御モジュール13
アクセス管理データベース15
データベース17
D
S141
S143
S145
S147
S149
S151
S153
A
NO
Yes
データ登録

【図8】



フロントページの続き

(72)発明者　坪井　俊明
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　中村　能章
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　橋本　聡
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　澤地　守
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5B017 AA01 AA04 BA05 BB02 CA16
5B075 KK43 KK54 KK63 PP06 PP13
PQ02 PQ46 UU26
5B082 EA12 GA16 GC04
5B085 AE06 AE12 AE23